In today’s digital world, many businesses are transforming into ecommerce systems to allow convenient shopping for customers. As much convenient as it is, it has also opened opportunities for cyber criminals to carry out various online crimes. Data breaches not only affect businesses, they also affect customers as their sensitive information can be misused for malicious purposes.

To protect their customers, business owners have to ensure that their payment systems are secure. The following are some ways in which online payment security can be observed by businesses:

1. **Always Use Two-Factor Authentication**

It is crucial to have two-factor authentication for online accounts, including social media, mobile banking applications, and ecommerce websites. This way, even if someone gets an access to your password, they will still need a second factor to authenticate payments. Two-factor authentication prevents hackers from conducting fraudulent payments on your behalf and secures your account. It also notifies the customer when someone tries to access your account from a new device. Businesses must ensure that they have two-factor authentication for approving any online payments on their website while a customer is making a purchase.

1. **Store Sensitive Information with a Third Party**

As a business that accepts credit cards for payments, never store credit card numbers of customers. In case of a hacking attempt on the data, cyber criminals should not be able to access your customer credit card numbers as it can cause your business a huge financial setback and reputational damage. By using a third-party transaction partner that specializes in storing and securing payment data, businesses can hand over the responsibility of storing payment details and ensure that their customer data is safe.

1. **Choose Secure E-commerce Platform**

If you are using an ecommerce platform for building your website, always choose a secure one, e.g., Shopify. This gives peace of mind along with added security. As a business owner, you will not have to be entirely responsible for detecting threats, but will also have a third party that can provide security and help you out.

1. **Get SSL Certificate for your Website**

Many small businesses think that hackers will not target them, and hence, they overlook security. This is why small businesses are easy targets when it comes to credit card breaches, and are targeted more than large businesses. Getting an SSL certificate for a website helps protect your website and sensitive information of customers.

1. **Buy Cyber Liability Insurance**

Since businesses are collecting personal information through online transactions, they are more at risk of financial implications in case of a data breach. Buying cyber liability insurance can help them to balance the financial impact of data breach incident and the associated legal costs.

1. **Use a Personal Verification System**

Among various [payment schemes](http://www.cardzgroup.com/ContactSmartCard.html), personal verification system allows customers to verify themselves with an identification document, such as a passport or driver’s license. Verified users are able to make immediate payments for a product or service without waiting for any confirmation.

1. **Don’t Collect Too Much Information**

It is important to only collect the required information from your customer when they are making a transaction and not collect more than what is needed. This cuts down the risks associated with a data security breach.

1. **Ensure PCI DSS Compliance**

The Payment Card Industry Data Security Standard (PCI DSS) provides a set of rules for the payment industry to comply with for ensuring secure payments. As a business that accepts online payments, it is highly recommended to comply with the PCI DSS standard to not only establish the trust of customers but also ensure that all measures are taken for providing maximum security of payments made through credit or debit cards.

1. **Ensure that your Hosting Provider Follows all Security Protocols**

As an ecommerce business, you not only need to ensure the safety of your website but also that of the hosting provider. To accept online payments securely, it is important that your web hosting provider also follows security protocols and has all necessary safeguards in place.

1. **Look for Patterns**

Employees should be trained to look for any fraudulent patterns during online purchases. Even with all security measures in place, every now and then a malicious transaction may take place and go unnoticed due to invigilance. Look out for these and train employees on how they can recognize and watch out for such patterns.

**Conclusion**

For businesses, opening an online store is no more an option but a necessity. Consumers today expect to be able to shop from the convenience of their homes any time from their phones and computers. They also want to ensure that they can conduct safe and fast transactions with their payment cards. Hence, it is important for businesses to ensure the safety of their customer’s financial and personal information and provide them with a convenient and pleasant online shopping experience by following best practices of online payment security.